Statement of Larry Todd
Director of Security, Safety, and Law Enforcement
U.S. Bureau of Reclamation
Before the
U.S. House of Representatives
Committee on Homeland Security
October 18, 2005

Mr. Chairman, my name is Larry Todd, and until recently I served as the Director of Security, Safety, and Law Enforcement for the U.S. Bureau of Reclamation. Established in 1902, Reclamation is known primarily for the dams, power plants, and canals we have built and operate in seventeen western States. Reclamation is our Nation's largest wholesaler of water, and its second largest producer of hydroelectric power. I am pleased to appear before you today to tell you about the security of the control systems used by the Bureau of Reclamation.

Reclamation's Supervisory Control and Data Acquisition (SCADA) Systems
Reclamation employs SCADA systems as tools to enable us to meet our mission obligations of providing essential services and commodities. These obligations include electric power generation, flood monitoring, water regulation, and water delivery. To accomplish these goals, Reclamation controls water release gates and valves at dams; hydroelectric generators, circuit breakers, switches and transformers at power plants; and pumps and gates on waterways and canals.

Reclamation's SCADA systems collect information about our facilities through transducers, converting information such as gate position, reservoir level, hydroelectric generator output, and water flow to electrical signals for processing in the SCADA system's computers. Once in the computers, the information is examined for any unusual characteristics, such as whether it exceeds an expected value. When information does not meet expectations, alarms may be triggered to inform operations staff of the situation, enabling them to take corrective actions. Reclamation's major SCADA control centers are manned at all times, enabling operations staff to react to both normal operations and emergency situations 24 hours a day and 365 days a year.

Along with collecting information, Reclamation's SCADA systems also facilitate our operations staff's reaction to normal and abnormal operational needs. They do this by supporting the supervised remote control of our facilities. By providing the operations staff with information about the facility, informed decisions can be made quickly and the appropriate actions taken. The SCADA systems computers help to supervise these decisions by ensuring that they meet safe operational criteria.

Protecting Reclamation's SCADA Systems
The focus of security efforts has changed since SCADA systems were first employed by Reclamation. In those early years SCADA design focused almost entirely on the operational integrity of the SCADA systems. In all cases where SCADA systems were permitted to control equipment, the safety and reliability of the control was examined and appropriate improvement measures were engineered and incorporated. This supported safer equipment operation and

permitted the disabling of SCADA control if necessary. This was done to protect the equipment and to ensure the safety of the public and Reclamation personnel in the event of a SCADA malfunction. These safety measures acted independently from the SCADA system to ensure that the failure of the SCADA system did not adversely affect the safety measures. If the safety of SCADA control actions could not be ensured, additional steps were taken to limit the degree of SCADA control or the control was not enabled. Reclamation still follows these practices in implementing its SCADA systems, providing a significant measure of operation security for its SCADA controlled facilities.

From the very beginning of Reclamation's use of SCADA systems, we have maintained a policy of not connecting our SCADA systems to our administrative networks. Today we adhere to that policy in all but the most unusual of situations. All connections to SCADA systems are minimized. Reclamation does not connect its SCADA systems to the Internet and routinely tests to ensure that such connectivity does not exist. Wherever practical, connections to our SCADA systems do not use Internet-like protocols, instead employing simple, limited capability, serial protocols. Those connections that must be present and that use Internet-like protocols are protected by firewalls and intrusion detection systems. Reclamation has adopted "best practices" and follows the cyber security guidance outlined by the National Institute of Standards and Technology (NIST) in their Special Publications.

In addition, Reclamation has evaluated and improved both personnel and physical security at our SCADA facilities. We perform background checks on key personnel and have "hardened" our facilities and control rooms through the addition of various access controls. This includes the access to our SCADA system control consoles.

To help identify physical and cyber vulnerabilities within the organization, Reclamation has invited independent organizations, including some represented by other panel members, to evaluate our security posture. We have also supported numerous investigations by our Inspector General's Office, some of which included limited penetration testing of our SCADA systems. The Inspector General's FY05 management report concluded that "the SCADA systems are operating in relative safety from potentially catastrophic cyber-security threats." To maintain these results, we are continuously evaluating and implementing prudent and practical security improvements.

Actions to Improve SCADA Security

Despite our security successes so far, Reclamation believes we can still take additional steps to improve the security of our SCADA systems. These steps, specifically identified and addressed in internal documents, will create more rigorous testing processes, improve and increase the frequency of security assurance reviews, and establish more comprehensive security planning targets. We also favor additional steps to improve the coordination of SCADA security efforts at both the Federal and private sector levels. Close coordination will assure consistency of Federal and private sector standards and security guidance, and could also help ensure that an appropriately rigorous security baseline is established for SCADA systems employed in different industry segments, depending on the significance of the infrastructure monitored or controlled.

In Summary

Reclamation recognizes that it plays a key role in protecting critical infrastructure components, including dams, waterways, water resources, and electrical generation capability. Where we employ SCADA systems to facilitate the control of these components, we believe we have taken responsible steps to ensure their security and safe operation. We recognize that cyber security, as it applies to both administrative and SCADA systems, requires continuous monitoring and diligence. We believe our security program meets the challenges of these requirements, but look forward to contributing to and employing better development, assessment, and protection tools and techniques as they become available.